PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-188782
(43)Date of publication of application : 24.07.1990

(51)Int.Cl. G09C 1/00
H04L 9/06
H04L 9/14

(21)Application number : 01-009582
(22)Date of filing : 17.01.1989

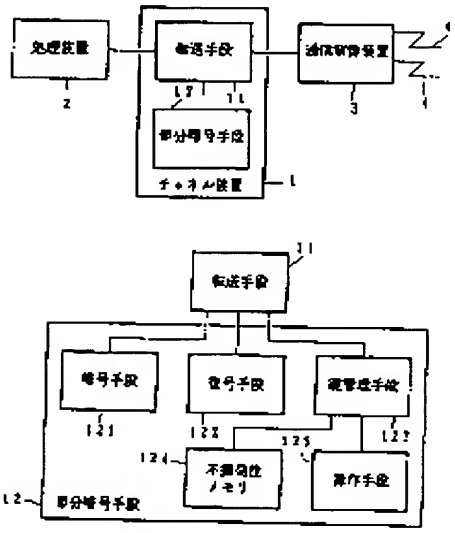
(71)Applicant : NEC CORP
(72)Inventor : UMEDA MASAO

(54) ENCIPHERING DEVICE

(57)Abstract:

PURPOSE: To reduce loads on a processor and a communication controller and to improve key control security by enciphering and deciphering a communication message for only a necessary part of transfer data by a channel device interposed between the processor and communication controller.

CONSTITUTION: The channel device 1 consists of a transfer means 11 and a partial enciphering means 12 and the transfer means 11 transfers the communication message between the processor 2 and communication controller 3. At this time, the partial enciphering means 12 executes partial enciphering and deciphering of the communication message. The partial enciphering means 12 is equipped with an enciphering means 121 which enciphers part of the transfer data transferred by the transfer means 11, a deciphering means 122 which deciphers the transfer data partially, and a nonvolatile memory 124 stored with a key for enciphering. Further, the device is equipped with an operation means 125 which sets and reads the key out from outside the device and a key control means 123 which sets the key with a command and takes the key out for enciphering and deciphering. Consequently, the key is controlled in safety without decreasing the CPU processing ability of the processor 2 or communication controller 3.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

出　願　特願平01-9582　(平 1. 1.17)

公　開　特開平02-188782　(平 2. 7.24)

公　告

登　録

名　称　暗号装置

抄　録　〔目的〕通信メツセージの暗号化復号化処理を転送データの必要部分だけに対して処理装置と通信制御装置との間に入つているチヤネル装置で行うことにより、処理装置及び通信制御装置の負荷軽減と鍵管理セキユリテイの向上とを図る。〔構成〕チヤネル装置１は転送手段１１と部分暗号手段１２とから構成され、転送手段１１は処理装置２と通信制御装置３との間で通信メツセージを転送する。このときに部分暗号手段１２で通信メツセージの部分的暗号化と復号化とが行われる。この部分暗号化手段１２は転送手段１１で転送される転送データの一部分に対して暗号化を行う暗号手段１２１と、転送データの部分的復号を行う復号手段１２２と、暗号用鍵を保存する不揮発性メモリ１２４とを備える。さらに装置外からの鍵の設定及び読出しを行う操作手段１２５と、コマンドから鍵の設定及び暗号復号化のための鍵の取出しを行う鍵管理手段１２３とを備えて構成される。これにより処理装置２または通信制御装置３のＣＰＵ処理能力を低下させずに、キーの管理を安全に行うことができる。

出願人　日本電気　(株)

発明者　梅田政夫

ＩＰＣ　G09C 1/00　H04L 9/06　H04L 9/14

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平2-188782

⑤Int.Cl.⁵	識別記号	庁内整理番号	⑬公開　平成2年(1990)7月24日
G 09 C 1/00		7368-5B	
H 04 L 9/06			
9/14			
		6945-5K　H 04 L 9/02　Z	

審査請求　未請求　請求項の数 1　(全4頁)

⑭発明の名称　暗号装置

⑳特　願　平1-9582
㉒出　願　平1(1989)1月17日

㉑発明者　梅田　政夫　東京都港区芝5丁目33番1号　日本電気株式会社内
㉑出願人　日本電気株式会社　東京都港区芝5丁目7番1号
㉔代理人　弁理士　井出　直孝

明　細　書

1. 発明の名称

暗号装置

2. 特許請求の範囲

1. 処理装置と、通信制御装置と、この処理装置とこの通信制御装置との間の経路に挿入され、データ転送手段を有するチャネル装置とを備えた計算機装置に含まれる暗号装置において、

上記チャネル装置に含まれ、

上記データ転送手段が転送するデータに含まれるメッセージの暗号化および復号化をこのデータに含まれる個別キーに基づき実行する暗号復号化手段と、

上記個別キーが操作で入力され、この個別キーを上記チャネル装置に固有のマスタキーに基づき暗号化する操作手段と、

この操作手段で暗号化された個別キーを保持するメモリ手段と、

上記データに含まれるコマンドに応じて上記メモリ手段から相当の個別キーを抽出して上記暗号復号化手段に与える鍵管理手段と

を備えたことを特徴とする暗号装置。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、コンピュータのセキュリティ手段に利用する。特に、通信暗号化復号化手段に関する。

〔概要〕

本発明は、チャネル結合による通信制御装置を有する計算機システムにおいて、

通信メッセージの暗号化復号化処理を転送データの必要部分のみに対して処理装置と通信制御装置との間に入っているチャネル装置で行うことにより、

処理装置および通信制御装置の負荷軽減と鍵管理セキュリティの向上とを図ることができるようにしたものである。

〔従来の技術〕

従来、この種の通信暗号化および復号化は処理装置（ホスト）または通信制御装置（フロントエンドプロセッサ）内で行われていた。

〔発明が解決しようとする問題点〕

このように従来例では、処理装置内または通信制御装置内で行うので、

(1) 暗号化復号化に際して処理装置または通信制御装置のＣＰＵ能力を使うことになり、オーバヘッドが増加する欠点と、

(2) 鍵ファイルが一般ファイルと同様のファイル装置（ディスク装置など）に格納されることになり、外部からの犯罪行為に対し十分なセキュリティが保障できない欠点と

がある。

本発明は、このような欠点を除去するもので、セキュリティが保障されかつ処理装置または通信制御装置のオーバヘッドの増大を招かない暗号装置を提供することを目的とする。

〔問題点を解決するための手段〕

本発明は、処理装置と、通信制御装置と、この処理装置とこの通信制御装置との間の経路に挿入され、データ転送手段を有するチャネル装置とを備えた計算機装置に含まれる暗号装置において、上記チャネル装置に含まれ、上記転送手段が転送するデータに含まれるメッセージの暗号化および復号化をこのデータに含まれる個別キーに基づき実行する暗号復号化手段と、上記個別キーが操作で入力され、この個別キーを上記チャネル装置に固有のマスタキーに基づき暗号化する操作手段と、この操作手段で暗号化された個別キーを保持するメモリ手段と、上記データに含まれるコマンドに応じて上記メモリ手段から相当の個別キーを抽出して上記暗号復号化手段に与える鍵管理手段とを備えたことを特徴とする。

〔作用〕

チャネル装置に暗号復号化手段を持たせる。これにより、処理装置および通信制御装置のＣＰＵ能力を十分に発揮させることができ、また、鍵の設定時を除けば鍵の所在はチャネル装置のみであり、チャネル装置を物理的に保護すれば鍵は安全に保管できる。鍵の設定はＭＴ媒体などの可搬媒体から行い、チャネル装置への設定時間帯を十分に保護すれば鍵の安全を保つことができる。

〔実施例〕

以下、本発明の一実施例を図面に基づき説明する。

第１図はこの実施例の全体構成を示すブロック構成図である。この実施例では、第１図に示すように、チャネル装置１は転送手段11と部分暗号手段12とから構成され、転送手段11は処理装置２と通信制御装置３との間で通信メッセージを転送する。このときに部分暗号手段12で通信メッセージの部分的暗号化と復号化が行われる。

第２図は部分暗号手段12の構成を示すブロック構成図である。この部分暗号化手段12は、転送手段11で転送される転送データの一部分に対して暗号化を行う暗号手段121 と、転送データの部分的復号を行う復号手段122 と、暗号用鍵を保存する不揮発性メモリ124 と、装置外からの鍵の設定および読出しを行う操作手段125 と、コマンドから鍵の設定および暗号復号化のための鍵の取出しを行う鍵管理手段123 とから構成される。ここで、鍵にはチャネル装置対応に一つ持つマスタキーとトランザクション対応に一つ持つ個別キーとがある。個別キーはマスタキーで暗号化されチャネル装置１内の不揮発性メモリ124 に保持される。不揮発性メモリ124 の内容は転送装置が持つコマンドでは読出すことができず、操作手段125 であるチャネル装置１の操作パネルからのみデバッグ時、保守時および試験時など十分な監視下で読出すことができる。

すなわち、この実施例は、第１図および第２図に示すように、処理装置２と、通信制御装置３と、この処理装置２とこの通信制御装置３との間の経路に挿入され、データ転送手段である転送手段11を有するチャネル装置１とを備え、さらに、本発明の特徴とする手段として、チャネル装置１に含まれ、上記データ転送手段が転送するデータに含

されるメッセージの暗号化および復号化をこのデータに含まれる個別キーに基づき実行する暗号復号化手段である暗号手段121 および復号手段122と、上記個別キーが操作で入力され、この個別キーをチャネル装置1に固有のマスタキーに基づき暗号化する操作手段123 と、この操作手段125 で暗号化された個別キーを保持するメモリ手段である不揮発性メモリ124 と、上記データに含まれるコマンドに応じて上記メモリ手段から相当の個別キーを抽出して上記暗号復号化手段に与える制御手段123 とを備える。

第3図は転送データの形式を示す図である。転送データは、通信メッセージ部と、メッセージの制御情報である通信ヘッダ部と、本発明の部分暗号化および復号化のための暗号ヘッダ部とから構成される。通信ヘッダ部は処理装置および通信制御装置内でのソフトウェアであり、メッセージを処理するための制御情報であり暗号化はしない。暗号化の対象となる部分は通信メッセージ部のみである。暗号ヘッダ部は転送データが暗号化または復号化されるときの個別キーを格納する部分である。

(本頁以下余白)

表

コマンド名	パラメータ
ライトマスタキー (Write Master Key)	マスタキー格納域アドレス、キーの長さ
ライトキー (Write Key)	個別キー格納域アドレス、キーの長さ、個別キーＩＤ
ライトメッセージ (Write Message)	メッセージ格納域アドレス、メッセージ長暗号復号位置、暗号復号指定
リードメッセージ (Read Message)	メッセージ格納域アドレス、メッセージ長暗号復号位置、暗号復号指定

(本頁以下余白)

表はチャネル装置1の持つコマンドの内の暗号関係のコマンドを示す。

ライトマスタキー(Write Master Key)は、チャネル装置1にマスタキーを設定するコマンドである。マスタキーは個別キーを暗号化して保持する暗号化キーである。

ライトキー(Write Key) は、トランザクションごとに使用される個別キーおよびメッセージ内で指定する個別キーＩＤをチャネル装置1内に登録するコマンドである。既に格納されている個別キーＩＤが指定されたときは以前の個別キーは新しい個別キーで置換される。

ライトメッセージ(Write Message) は、メッセージをチャネル装置1に送出するコマンドである。送出するときのパラメータとしては、メッセージ格納域アドレスと、メッセージ長の他に暗号復号処理を開始するメッセージ上の位置と、暗号するか復号するかの区別のパラメータとがある。暗号復号位置は通常通信メッセージの開始位置を指定する。

リードメッセージ(Read Message)はメッセージを受取る処理であること以外はライトメッセージと同じコマンドである。

暗号化および復号化はリードおよびライトのいずれの時点でも可能である。

〔発明の効果〕

本発明は、以上説明したように、チャネル装置上で通信メッセージを暗号化するので、処理装置または通信制御装置のＣＰＵ処理能力を低下させない効果がある。また、暗号キーの格納場所が一般のファイル装置上ではないので、通常のユーティリティプログラムなどでは読出すことができず、キーの管理を安全に行える効果がある。

4. 図面の簡単な説明

第１図は本発明実施例の全体構成を示すブロック構成図。

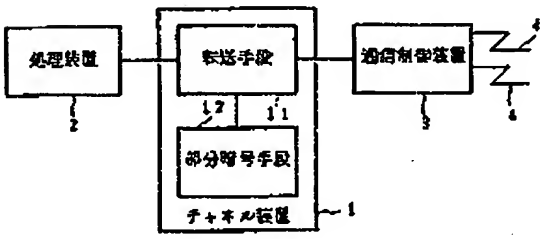
第２図は本発明実施例の部分構成を示すブロック構成図。

第３図本発明実施例で転送される転送データの形式を示すフォーマット図。

１…チャネル装置、２…処理装置、３…通信制御装置、４…回線、11…転送手段、12…部分暗号手段、121 …暗号手段、122 …復号手段、123 …鍵管理手段、124 …不揮発性メモリ、125 …操作手段。

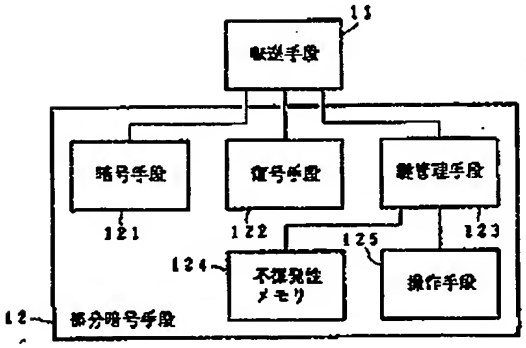
特許出願人　日本電気株式会社

代理人　弁理士　井出直孝



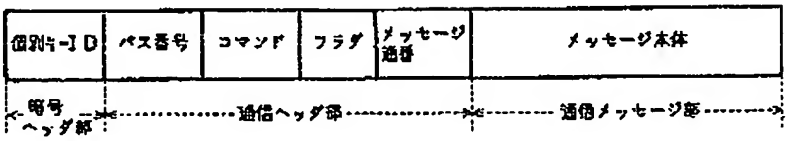
実施例の構成

第　１　図



部分暗号手段の構成

第　２　図



転送データの形式

第　３　図